



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

July 23, 2015

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

**ADVISORY NUMBER:
SA2015-085**

**DATE ISSUED:
07/22/2015**

**SUBJECT:
Multiple Vulnerabilities in Internet Explorer Could Allow Remote Code Execution**

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer. The vulnerabilities could allow an attacker to execute code in the context of the browser. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed attempts will result in denial of service conditions.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

RISK:
Government:

- Large and medium government entities: High
- Small government entities: High

Businesses:

- Large and medium business entities: High
- Small business entities: High

Home users: High

TECHNICAL SUMMARY:

Microsoft Internet Explorer is prone to multiple vulnerabilities that could allow remote code execution. The vulnerabilities are as follows:

- Multiple use-after-free vulnerabilities occur when handling "CTreePos", "CCurrentStyle", " and "CAttrArray" objects.
- An out-of-bounds memory corruption vulnerability affects the 'CTableLayout::AddRow()' object due to the way that arrays representing cells in HTML tables are processed.

These vulnerabilities could allow an attacker to execute remote code by luring a victim visit a malicious website or open a malicious file. When the website is visited, the attacker's script will run within the context of the affected browser or with same permissions as the affected user account. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed attempts will result in denial of service conditions.

There are currently no patches available.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Configure Internet Explorer to prompt before running Active Scripting or disable Active Scripting in the Internet and Local intranet security zone until a patch is released.
- Once a patch is released by Microsoft, update immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.

REFERENCES:

TippingPoint Zero Day Initiative:

<http://www.zerodayinitiative.com/advisories/ZDI-15-359/>

<http://www.zerodayinitiative.com/advisories/ZDI-15-360/>

<http://www.zerodayinitiative.com/advisories/ZDI-15-361/>

<http://www.zerodayinitiative.com/advisories/ZDI-15-362/>

Security Focus:

<http://www.securityfocus.com/bid/75976>